Journal of The Korea Society of Computer and Information
Vol. 19, No. 11, November 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.11.097

분석단계에서 접근 통제의 보안 요건 정의

신 성 윤*

The Definitions of Security Requirements for Control Access on the Step of Analysis

Seong-Yoon Shin *

요 약

접근 통제란 기록과 기록이 담고 있는 정보를 보호하기 위하여 기록에 대한 접근을 제한하거나 허용하는 기록 관리 과정을 말한다. 본 논문에서는 업무수행자인 사용자의 역할과 데이터 사용행위를 기반으로 한 접근 및 권한 통제가 이루어져야 한다는 점을 강조한다. 조직의 운명을 좌우하는 매우 중요한 정보의 대량 조회 및 변경 작업은 반드시 사전 결재를 취득해야 가능하다는 점도 제시한다. 또한, 일정한 시간 동안 아무런 행위도 하지 않는 세션에 대하여 통제를 하는 것은 당연하다는 것도 제시한다. 그리고 접근 통제에 대한 보안 요건에 관한 사례를 직접 들어 설명하도록 하였다.

▸ Keywords : 접근 통제, 권한 통제, 조회 및 변경, 세션, 보안 요건

Abstract

The access control means the process to record and manage access restrictions and permits for protecting information in records. This paper emphasizes the control of access and authorization based on the roles and the data using activities of users as task performers. Also, it requires to gain the necessary approval in advance for important tasks such as mass inquiry and change on important information to influence the very existence of the whole organization. And then, it suggests that it is necessary to control some session of information with non-activity for certain time. Generally, this paper is to explain security elements of access control through various cases.

▸ Keywords : Access Control, Authority Control, Inquiry and Change, Session, Security Requirements

•제1저자 : 신성윤
•투고일 : 2014. 8. 12, 심사일 : 2014. 9. 12, 게재확정일 : 2014. 10. 8.
* 군산대학교 컴퓨터정보공학과(Dept. of Computer Information Engineering, Kunsan National University)

I. 서 론

접근 통제란 시스템과 네트워크 자원에 시도되는 허가되지 않은 접근에 대응하기 위한 첫 번째 방어수단 중 하나로서 접근을 승인하거나 거부함으로써 비 인가자에게 불법적인 자원 접근 및 파괴를 예방하는 하드웨어적, 소프트웨어적, 그리고 행정적인 관리를 말한다[1].

접근 통제 관련 연구로는, [2]에서는 기존의 DBMS 접근 통제 시스템의 구현 방식과 기능 연구, 한계점 분석, 개선방안 도출을 통해 개인정보보호법을 준수할 수 있는 효과적인 DB의 보안 접근 통제 시스템을 제시하였다. [3]에서는 의료정보 유출 방지를 위하여, 현행 네트워크 접근 통제 시스템을 개선 및 적용한 네트워크 이중 접근 통제 모델을 제시하였고, [4]에서는 접근 통제의 전반에 관한 것을 다룬 IHE(Integrating the Healthcare Enterprise)의 IT 인프라 기술 프레임 워크 백서를 발간하여 접근 통제의 기반을 다졌다. [5]에서는 원칙적 보안을 제공하면서 사용자의 정신 모델에 맞게 디자인 된 액세스 제어와 분산 파일 시스템인 Penumbra를 제시하였으며, [6]에서는 격자 모델 제시와 형식 매핑 및 구현 아이디어 및 연습에 이 방법의 문제에 대해 설명하는 동적이면서 유연하고 낙관적인 접근 통제를 제시하였다. 이 밖에도 RFID와 내부 위협에 의해 무단의 액세스로 인해 정보 유출 차단 및 인원 보안 강화에 대한 적외선을 결합 하여 네트워크 그룹 액세스 제어 시스템 제안[7], 내부 네트워크에 접속을 허가 받은 이가 인가된 장비를 이용하여 접근정책에 따른 통신을 수행하고 있는지를 확인하기 위한 연구로서 RFID 출입통제시스템과 연동한 네트워크 이중 접근통제 시스템을 제안[8], 접근제어 측면에서 유비쿼터스 컴퓨팅 환경을 정의하고 그 환경에서 접근제어의 특성을 분석한 뒤, 그 환경을 위한 접근제어 모델을 개발할 때 필수적으로 고려해야할 요구사항을 제시[9], 개방형 인증 프로토콜과 가상화 기술을 접목하여 사용자 권한에 따른 응용 소프트웨어를 제공하는 방안을 제안[10], 메시지통제시스템의 우회 접근 통제 모델을 제시하고 이를 사용하여 메시지의 유용성과 가용성을 높여줄 수 있는 웹기반의 메시지통제시스템[11] 등 다양한 분야의 접근 통제 시스템들을 제시하고 있다.

본 논문에서는 [2-11]과 같이 특정한 분야의 접근 통제를 다루지는 않고 어플리케이션 구현 단계 중 분석 단계에서 접근통제에 대한 요건을 정의하도록 한다. 이에 따라 본 논문의 구성 또한 2장에서는 접근 통제를 위한 원칙에 대해 논하고, 3장에서는 접근 통제를 위한 정의에 대해서 논하도록 한다. 그리고 4장에서는 어플리케이션 접근 통제와 IT 인프라 접근 통제에 대해서 논하도록 하며, 5장에서 이러한 접근 통제의 구현 방법 제시를 사례를 들어 설명하도록 하며, 6장에서 결론을 맺도록 한다.

II. 접근 통제의 원칙

접근에는 서로 상반되는 2가지 측면이 있는데, 첫째는 접근 통제를 통하여 기록과 그 속의 정보를 보호하는 것이고, 둘째는 이용자가 기록에 접근할 기회를 최대한 제공하여 기록의 이용을 촉진하는 것이다. ISO 15489가 제시하는 접근의 3가지 원칙은 다음과 같다[12].

① 누가 어떤 환경에서 기록에 접근하도록 허가할지를 규정하는 공식적인 지침이 있어야 한다.
② 효과적으로 접근을 통제하려면 기록과 개인 모두에게 접근 조건을 부여해야 한다.
③ 기록에 시의 적절하고 효과적으로 접근하여 검색할 수 있도록 해야 한다.

이렇게 국제 표준화 위원회에서 제시한 원칙에 따라서 우리는 다음과 같이 접근 통제의 원칙을 설정하였다.

첫째, 시스템의 사용은 명확히 설계된 권한에 의해서 제한되어야한다는 것이다.

둘째, 시스템 사용을 위한 주체, 객체, 행위가 정의되고 식별되어야 한다는 것이다.

셋째, 사전에 합의된 접근 제어 룰에 의해서 접근 및 사용이 통제되어야 한다는 것이다.

우리가 정한 접근 통제의 원칙은 조금 다르지만 국제 표준화 위원회의 원칙과 거의 같다고 볼 수 있다.

예를 들면 서버 관리자에게는 개발 시스템에 대한 접근권한을 줄 필요는 없고 역으로 프로그램 개발자에게는 서버의 운영권한을 줘서는 안 된다는 말이다. 이것은 세 가지 모두 적용된 원칙의 예이다.

III. 접근 통제를 위한 정의

정보 자산의 공개 및 노출, 위변조 및 파괴, 지체 및 재난 등의 위험으로부터 보호하여 정보의 기밀성, 무결성, 가용성을 확보하는 것이 정보 보호이다. 학술적으로는 정보시스템 내부에 보관되거나 통신망으로 전송되는 정보를 시스템 내부와 외부에 존재하는 각종 위험으로부터 안전하게 보호하여 정보시스템의 가용성을 보장하는 것이 정보 보호이다. 그리고

법적으로는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 수단을 강구하는 것이 정보 보호이다.

이러한 정보 보호의 3가지 정의인 기밀성, 무결성, 가용성에 대하여 다음과 같이 정의할 수 있다.

첫째, 기밀성(Confidentiality)이란 정보의 비밀이 누설되지 않고 지속적으로 유지되는 것을 말한다. 이는 반드시 허가된 객체에게만 정보가 제공되어야하며, 비인가된 객체로부터는 완벽히 차단 통제되어야 한다. 일반적으로 접근통제와 암호화를 통해 차단이 통제된다.

둘째, 무결성(Integrity)이란 허가되지 않는 객체로 부터 정보의 위변조 및 삭제 등을 막는 것을 뜻한다. 이는 정보의 정확한 전달과 안정을 보장하는 것이다.

셋째, 가용성(Availability)이란 서비스가 계속 유지가 되어 허가된 객체에게 정보가 제공되는 것을 의미한다. 이는 혹시 모를 공격에 대비하여 정보를 백업시키거나 의심스러운 위험 요소로부터의 보호를 통해 보장된다.

정보 보호를 위한 3가지 정의를 우리는 보안의 3요소라고 한다.

접근 통제를 위한 정의를 보면 사용자의 계정(ID)의 발급, 운영, 변경, 폐기를 위한 시스템의 보안 요건을 내부 어플리케이션, 외부 어플리케이션 및 IT 인프라로 나누어서 다음의 기준에 따라 정의할 수 있다. 정보 보호의 3가지 정의는 기본적으로 베이스에 깔려있다고 보는 것이 맞을 것이다.

① 사용자 유형 정의 : 사용자 별로 인증 수단 부여 및 어떠한 직원인지에 따라 접근 통제 권한 부여(그림 1)

인증수단	유형1	유형2	유형3	유형4
내부 직원	현업 직원	창구 직원	IT 부서 개발	IT 부서 운영
협력조직 직원	아웃 소싱 직원	n/a	n/a	m/a
시스템 사용자	미들웨어	DB	n/a	n/a

그림 1. 사용자 유형 정의 사례
Fig. 1. Case of Definition of User Type

② 정보의 등급 지정 : 유형별 신상 정보에 따라 정보의 등급을 세분화(그림 2)

유형	성격	예시	1등급	2등급	3등급
유형1	실명 확인 정보	주민 등록 번호	금융 거래 승인 및 본인 승인 핵심 정보 (예: 계좌 비밀 번호, 패스 워드 등)	본인 확인 및 계좌 확인 중요 정보 (예: 주민 번호, 계좌 번호)	1등급, 2등급 외 일반 정보 및 업무 처리 정보 (예: 주소, 이메일, 거래 내역)
유형2	신상 정보	이름, 주소, 전화 번호, 생일, 가족			
유형3	거래/ 신용 정보	아이디, 계좌 번호, 거래 내역			
유형4	비밀 번호	계좌 비밀 번호, 패스 워드			

그림 2 정보의 등급 지정 사례
Fig. 2. Case of Appointment of Information Class

③ 시스템 & 네트워크 등급 지정 : 시스템과 네트워크를 위치, 업무, 그리고 유형에 따라 세부적으로 지정(그림 3)

유형	Type A	Type B	Type C
위치	DMZ	내부망	내부망
업무	거래처리	업무연계	채널
유형	운영 시스템	운영 시스템	개발 시스템

그림 3 시스템 & 네트워크 등급 지정 사례
Fig. 3. Case of Appointment of Class on System & Network

IV. 어플리케이션 접근 통제와 IT 인프라 접근 통제

접근 통제 정책에는 임의적 접근 통제 정책, 강제적 접근 통제 정책, 그리고 역할 기반 접근 통제 정책이 있다.

임의적 접근 통제 정책은 객체에 근접하려고 하는 주체의 접근 권한에 따라 접근 통제를 적용하는 방이다. 이 방식은 사용자가 접근 권한을 자의적으로 추가하거나 및 회수가 가능한 방법이다. 또한, 데이터의 소유자가 마음대로 사용자 (그룹)의 신분에 따라 임의로 접근을 통제할 수 있다.

강제적 접근 통제 정책은 객체에 포함된 정보의 비밀성과 이러한 비밀성의 접근 정보에 대해 주체가 갖는 권한에 근거하여 객체에 대한 접근을 제한하는 방법이다.

역할 기반 접근 통제 정책은 임의적 접근 통제 정책의 단점을 개선한 방법으로 비임의적 접근통제라고도 한다. 이 방법은 사용자에게 최소한의 권한을 부여함으로써 권한의 오용과 남용을 방지할 수 있다.

본 논문에서는 이러한 접근 통제 정책들을 바탕으로 조직/그룹/직무 등에 따라 사용 주체를 정의하고, 어플리케이션 화면에서 제공하는 서비스를 정의하여 Role 기반으로 이루어지도록 하며, 사용 행위에 따라 좀 더 세부적인 통제가 이루어지도록 설계한다.

그림 4에서는 사용자 주체에 따른 Role 정의의 예시를 나타냈고 그림 5에서는 사용 행위 Type의 예시를 나타내고 있다.

사용자/조직/그룹/직무		
level 1	level 2	level 3
임원	지점영업	일반주문
부서장	본사일반	지점전직원
지점장	본사영업	부실장전용
지점업무팀장	본사관리	부실점장전용
지점업무직원	본사업무	지점업무팀장전용

그림 4. 사용자 주체에 따른 Role 정의 사례
Fig. 4. Case of Role Definition of User Main Subject(Example)

서비스		Action Type										
서비스 ID	설명	조회		입력	수정	삭제	다운로드		인쇄		
		대량	마스킹				대량	마스킹	화면	기능	마스킹
KIS061032001	임원전용 서비스 001	V		V	V	V	V		V		V
KIS061022001	주문정보 조회 001	V	V					V		V	
KIS061021001	공지사항 001		V	V	V	V		V	V	V	

그림 5. 사용 행위 타입 사례
Fig. 5. Case of Act Type of Usage

IT 인프라 접근 통제란 서버, 데이터베이스, 그리고 네트워크에 대한 접근 통제를 말한다. 서버란 네트워크에 연결된 다른 컴퓨터에 서비스를 제공하기 위한 컴퓨터 또는 소프트웨어를 가리키는 말이다. 반대로 서버에서 보내 주는 정보 서비스를 받는 쪽이나 요구하는 쪽의 컴퓨터 또는 소프트웨어를 클라이언트라고 한다. 데이터베이스는 어떠한 조직 내에서 다수의 사람에 의해 공유되어 사용되어질 목적으로 컴퓨터가 접근할 수 있는 장치에 통합적으로 조직되고 관리되는 운영 자료의 집합을 말한다. 그리고 네트워크는 하나의 통신망을 뜻하며, 데이터 통신이라는 하나의 목적을 기반으로 하여 두 개 이상의 장치들이 연결되어 있는 통신 구조를 말한다. 그림 6에서는 IT 인프라 등급별 접근 통제 설정의 예를 설명하고 있다.

종류	IP 통제	클라이언트 프로그램 제한	추가 인증 실시
운영 시스템 (외부)	OK	OK	OK
운영 시스템 (내부)	OK	OK	-
개발 시스템	-	-	-

그림 6. IT 인프라 등급별 접근 통제 설정 사례
Fig. 6. Case of Set of Access Control from IT Infra Class

데이터베이스 컨트롤에서 보안 요구 사항은 정당한 사용자의 데이터 접근 지원, 추론 방지, 데이터의 무결성 유지, 데이터 의미(Semantic) 무결성 유지, 시스템 감사, 사용자 인증, 기밀 데이터 관리와 보호, 다단계 보호(Multilevel Protection), 감금(Confinement) 등이 있으며, 이벤트 처리에는 바람하지 않은 이벤트 회피, 이미 발생한 이벤트 식별, 이미 발생한 바람직하지 않는 이벤트 교정, 보안 위반 잠재우기, 자원과 기능을 복구, 다른 통제 기법으로 대체 등으로서 예방, 탐지, 교정, 억제, 복구, 대체 등에 해당되는 접근통제 방법이다.

V.구현의 방법 제시 및 결과

본 논문에서는 구현의 방법 제시로서 ○○○○사의 분석 단계의 보안 요건 정의에서 접근 통제에 대한 구현 방법 제시 사례를 들었다. 그림 7은 접근 통제에 대한 보안 요건의 정의에서 사용 주체에 따른 접근 통제의 구현 방법 제시이며 그림 8은 사용 행위에 따른 권한 관리 구현 방법 제시 사례이다.

요건 ID	요건 명	Num	상세 요건
00-00-01	사용 주체에 따른 접근 통제	1	통합인증을 통해 업무 시스템 접근 권한을 통제
		2	사용자, 조직/그룹 등 사용 주체를 식별하고, 직무 분류를 통해 정의된 역할에 따라 시스템, 메뉴/화면/서비스 별로 접근 권한을 부여 - 직무 분류에 의한 사용 주체 정의 : AS-IS 분석을 통해 도출 업무별 필요한 최소 접근 권한을 부여
		3	관리자는 지정된 터미널에서만 접근이 가능하도록 함
		4	관련 로그를 생성 1. 로그 생성 시기 : 관리자에 의한 권한정보 변동 시 2. 로그 포함 항목 : 시간, 대상자, 관리자 ID, 변동된 권한 정보 등 3. 로그 보관 주기 : 5년
		로그	권한 변경 내역 보고서를 작성 1. 접근 권한 관리 목록, 권한 관련 변동 내역 레포트

그림 7. 사용 주체에 따른 접근 통제 구현 방법
Fig. 7. Implementation Method of Access Control from Subject of Usage

요건 ID	요건 명	Num	상세 요건
00-00-02	사용 행위에 따른 권한 관리	1,2	해당 업무 화면내 데이터 사용 행위(처리)에 따라 레벨별 적절한 권한을 관리 - 사용 행위에 대한 허가 권한은 해당 데이터의 오너쉽을 가진 부서장 또는 결재권자가 가짐 데이터 사용 행위는 기존 조회, 변경 행위를 포함하여 아래와 같이 정의한다. - 조회(R) : 데이터를 Read 하는 것을 의미 - 변경 : 데이터에 대한 입력(C), 수정(U), 삭제(D)를 의미 - 다운로드 : 데이터를 해당 데이터베이스 외의 다른 장소(개인 PC 등)로 복사(다운로드) 하는 것을 의미 - 화면 인쇄 : Print Screen과 같이 조회된 화면을 인쇄하는 것을 의미 - 기능인쇄 : 특정 양식 및 보고서 출력 등 업무시스템(어플리케이션)에 구현된 인쇄 기능을 활용하여 인쇄하는 것을 의미
		3	고객 정보 50건 이상의 다운로드, 인쇄 시는 로그를 생성 1. 로그 포함 항목 : 일시, 사번, IP 주소, 인쇄/다운로드 된 정보(화면 번호, 화면 명 (예: 계좌정보조회))
		로그	관련 로그를 생성한다. 1. 로그 생성 시기 : 데이터의 조회, 변경, 다운로드, 인쇄 등의 권한 부여/변경/삭제 시 2. 로그 포함 항목 : 시간, 대상자, 관리자 ID, 변경된 권한 정보(사용 행위) 등 3. 로그 보관 주기 : 5년

그림 8. 사용 행위에 따른 권한 관리 구현 방법 사례
Fig. 8. Example of Authority Management Implementation Method from Act of Usage

또한 그림 9는 세션 관리의 구현 방법의 사례이고, 그림 10은 출력 및 복사 시 보호 조치에 관한 구현 방법의 사례를 나타내고 있다.

요건 ID	요건 명	Num	상세 요건
00-00-01	세션 관리	1	동일한 계정의 멀티 세션 연결을 제한(직원)
		2	사용이 종료돈 후에 자동적으로 세션을 종료

그림 9. 세션관리 구현 방법의 사례
Fig. 9. Example of Session Management Implementation Method

요건 ID	요건 명	Num	상세 요건
00-00-02	출력 및 복사 시 보호 조치	1	인쇄물을 출력 시 워터마킹 적용 - 로고, 일시, IP, 성명 등 표시 - 통장 프린터, 공문 발송 등은 업무 특성상 적용되지 않음
		2	어플리케이션 화면에 대한 캡쳐/복사 방지 기능을 적용 - 서버 DRM 적용 - 2등급 데이터
		로그	인쇄 출력 관련 로그를 생성 1. 로그 생성 시기 : 인쇄물 출력 시 2. 로그 포함 항목 : 일시, IP, 사번, 항목 등 3. 로그 보관 주기 : 1년

그림 10. 출력 및 복사시 보호 조치에 관한 구현 방법 사례
Fig. 10. Example of Protective Measure Implementation Method at Print and Copy

이상에서 다룬 접근 통제의 원칙, 정의, 어플리케이션 접근 통제, IT 인프라 접근 통제를 바탕으로 10개의 중소기업을 대상으로 구현 방법을 제시한 결과 정보 보호의 3가지 정의인 기밀성, 무결성, 가용성 등이 그림과 같이 향상되어 나타나는 것으로 볼 수 있다.

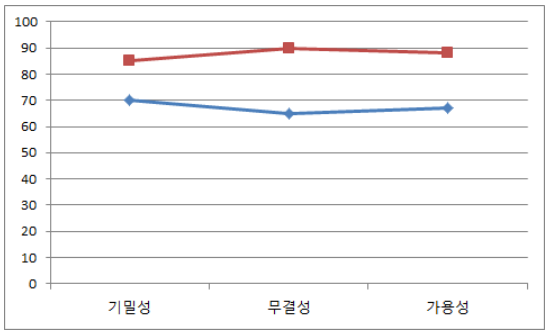

그림 11. 정보 보호의 향상
Fig. 11. Enhancement of Information Protection

그림 11에서 아래의 선분은 기존의 접근 통제 방법으로 알아본 정보 보호의 형태이고, 위의 선분은 제시한 접근 통제를 바탕으로 구현한 경우의 정보 보호의 형태이다.

Ⅵ. 결 론

접근 통제는 보안의 3요소인 자원에 대한 기밀성, 무결성, 가용성과 이들의 합법적인 이용과 같은 정보보호 서비스에 대한 권한 부여를 위한 수단이다. 즉, 접근 통제는 자원에 대하여 비인가된 접근 감시, 접근 요구 이용자 식별, 접근 요구의 정당성 확인 및 기록, 보안 정책을 바탕으로 접근 승인 및 거부로써 비인가자에 대한 위법적이고 불법적인 접근 및 파괴를 방지하는 하드웨어, 소프트웨어, 행정적인 업무 관리 전반을 말한다.

본 논문에서는 업무를 수행하는 자인 주체적인 사용자의 역할과 데이터 사용행위를 바탕으로 한 접근 통제와 권한 통제가 이루어져야 한다는 점을 제시하였다. 상당히 중요한 정보를 대량으로 검색 및 조회하거나 수정 및 변경하는 작업은 반드시 사전 결재를 득한 후에 가능하다는 것도 제시하였다. 또한, 접근통제의 원칙과 정의에 대하여 설명하였고, 어플리케이션 접근 통제와 IT 인프라인 서버, 데이터베이스, 그리고 네트워크에 대한 접근 통제는 예를 들어서 직접 설명하였으며, 구현의 사례로서 한 기업의 접근통제에 대한 보안 요건의 정의를 실례로서 설명하였다.

참고문헌

〔1〕 http://flyingwolf.co.kr/110185021556
〔2〕 Jong-Il Baek, "Access Control Security Technology for the Protection Vulnerable DB Objects, Department of IT Application Technology, The Graduate School of Venture, Hoseo University, 2012
〔3〕 Kyong-Ho Choi, Sung-Kwan Kang, Kyung-Yong Chung, Jung-Hyun Lee, "A Study of Network 2-Factor Access Control Model for Prevention the Medical-Data Leakage," Jouranl of Digital Convergence, Vol. 10, No. 6, pp. 341-347, 2012
〔4〕 Jörg Caumanns, Raik Kuhlisch, Oliver Pfaff, Olaf Rode, "IHE IT Infrastructure Technical Framework White Paper - Access Control," IHE International, 2009
〔5〕 Michelle L. Mazurek, Yuan Liang, William Melicher, Manya Sleeper, Lujo Bauer, Gregory R. Ganger, Nitin Gupta, and Michael K. Reiter, "Toward strong, usable access control for shared distributed data," FAST'14 Proceedings of the 12th USENIX conference on File and Storage Technologies, PP. 89-103, 2014
〔6〕 Peisert, Sean, and Matt Bishop. "Dynamic, flexible, and optimistic access control." Dept. of Computer Science, University of California at Davis, Davis, CA, USA, Technical Report CSE-2013-76, 2013
〔7〕 JongMin Kim, KyongHo Choi, DongHwi Lee, "Network Group Access Control system using piggy-backing prevention technique based on Infrared-Ray," Journal of Korea Convergence Security Association, Vol. 12, No. 4, pp.109-114, 2012
〔8〕 KyongHo Choi, JongMin Kim, Daesung Lee, "Network 2-Factor Access Control system based on RFID security control system," Journal of Korea Convergence Security Association, Vol. 12, No. 6, pp. 53-58, 2012
〔9〕 Park HM, Lee YL, Lee HH, "Analysis of Access Control Model for Ubiquitous Computing," Review of KIISC Vo. 19, No. 2, 2009
〔10〕 Sun-Joo Kim, In-June Jo, "Access Control Method for Software on Virtual OS Using the Open Authentication Protocol," The Journal of

the Korea Contents Association, Vol. 13, No. 12, pp. 568-574, 2013
〔11〕 Young-soo Kim, Sun-goo Jo, "Indirection based Multilevel Security Model and Application of Rehabilitation Psychology Analysis System," J. Korea Inst. Inf. Commun. Eng., Vol. 17, No. 10, pp. 2301~2308, Oct. 2013
〔12〕 http://terms.naver.com/entry.nhn?docId =441192&cid =442&categoryId=442

저 자 소 개

신 성 윤
2003년 2월 군산대학교 컴퓨터과학과 이학박사
2006년~현재 : 군산대학교 컴퓨터정보공학과 교수
관심분야 : 영상처리, 컴퓨터비전, 가상현실, 멀티미디어
Email : s3397220@kunsan.ac.kr